Contents lists available at ScienceDirect

Process Safety and Environmental Protection

journal homepage: www.elsevier.com/locate/psep

The role of component arrangement in complex safety instrumented systems—A case study

*Hamid Jahanian**, *Adam Lucas*[1]

Siemens Ltd., Energy Sector, 160 Herring Road, Macquarie Park, NSW 2113 Australia

ARTICLE INFO

Article history:
Received 26 August 2014
Accepted 29 December 2014
Available online 20 January 2015

Keywords:
Complex safety instrumented systems
SIS component arrangement
Model uncertainty
PFDavg
SIS
Safety systems optimization

ABSTRACT

The arrangement of components plays a key role in the performance of complex Safety Instrumented Systems (SIS), in which a SIS logic solver is interlocked with other logic solvers, to share a final element, for instance. The position of the components and the way they are utilized affects the reliability characteristics, such as the Probability of Failure on Demand (PFD), Spurious Trip Rate (STR), architectural sensitivity and model uncertainty. This case study uses quantitative and qualitative approaches to elaborate on various aspects of component arrangement in complex SIS. Numerous simplified models are analyzed; new classification is introduced for SIS components based on their response to demand; a set of guidelines are developed for SIS architecture design, with a focus on component arrangement; and the use of these guidelines is demonstrated in a real-life example, where an existing turbine SIS is modified to incorporate a new over-speed protection system. The simplified models and the turbine upgrade project are also used to explain the issue of unknowns and uncertainties in reliability analysis and how these issues can be addressed in SIS architecture by optimizing component arrangement.

1. Introduction

Safety Instrumented Systems (SIS) do not always follow the classic model of sensor – logic solver – final element. This model is surely the most logical solution: a set of sensors to detect the process hazard; a logic solver to make a decision if an emergency shutdown is required; and a set of final elements to isolate the process from the hazard. Seemingly, there is no need to add further complexity to this simple, logical and working model. However, one may always encounter more complex SIS architectures where the combination of SIS subsystems cannot be established as simple as the classic model, for various engineering reasons.

This paper presents a case study on one form of complexity in safety systems, where a SIS consists of multiple logic solvers, each performing a separate set of Safety Instrumented Functions (SIFs), yet all driving the same final element. A simplified block diagram of such a SIS configuration with two logic solvers and one final element is shown in Fig. 1. In this figure, the sensor S1, the logic solver LS1, and the final element F form one safety function, SIF#1; and the sensor S2, the logic solver LS2 and the same final element, F, form another safety function, namely SIF#2. Both SIF#1 and SIF#2 drive the same final element, as they are both intended to protect the same process.

A puzzling design issue in complex SIS architectures is finding the optimum arrangement of SIS components. There may be more than one way to interface between the sensors, logic solvers and final elements, depending on which the collective performance of the SIS can be different. What sensors should be wired to each logic solver? Which logic solver should physically drive the final element? Do the CPUs need to communicate to each other, or should they work independently? How should we calculate the Probability of Failure on Demand

* Corresponding author. Tel.: +61 408473423.
E-mail addresses: hamid.jahanian@siemens.com (H. Jahanian), adam.lucas@siemensppa.com.au (A. Lucas).
[1] Tel.: +61 403430869.
http://dx.doi.org/10.1016/j.psep.2014.12.009
0957-5820/

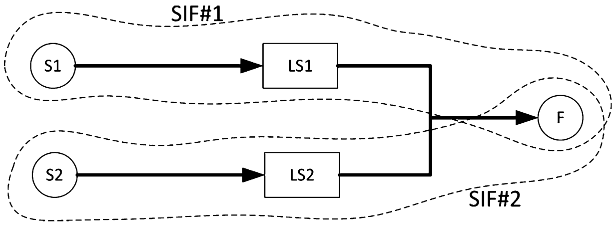

Fig. 1 – SIS with multiple logic solvers.

(PFD), and how can we minimize it? How is the Spurious Trip Rate (STR) affected by the arrangement of the components? What are the impacts of the safety system on the Basic Process Control System (BPCS)? What are the characteristics that we should try to optimize when we design the SIS arrangement? These are some of the questions that one would need to answer when designing complex SIS architectures.

Section 2 of this paper begins examining the role of component arrangement in complex SIS by comparing twenty-five simplified models. The models present various possible combinations of SIS subsystems in applications with more than one CPU. The analysis is developed further in Section 3 by introducing a new classification of SIS components based on their functions in responding to demands. This classification is then used as the basis for a set of design guidelines, explained in Section 4. These general guidelines can assist safety engineers in designing optimum architectures for complex SIS. Using the findings in Sections 2–4, Section 5 details a real-life application of a turbine upgrade project, in which two proposed solutions for a new SIS architecture are compared from both qualitative and quantitative perspectives to demonstrate the role of component arrangement in complex SIS architectures, and explain how this role can affect the overall reliability of the system.

2. Simplified models

This section analyzes the role of component arrangement by using simplified models of complex SIS, and comparing various combinations of sensors, logic solvers, interface elements and final elements. The models in this section, referred to as Simplified Models, are divided into four groups:

1. Configurations with one SIS logic solver
2. SIS logic solvers interlocked with BPCS logic solvers
3. Configurations with two SIS logic solvers
4. BPCS logic solver interlocked with two SIS logic solvers

Except for the first group, which includes the classic SIS configuration, each Simplified Model in the other three groups consists of a SIS logic solver that shares the final element with other SIS and/or BPCS logic solver(s). Each logic solver is connected to its own sensor and processes either a safety function (if of SIS type) or a control function (if of BPCS type). The final element is shared between the logic solvers, instigating architectural complexity on which the analysis in this section is focused.

Graphical representations of the Simplified Models, as well as two tables for the typical failure rates of the components and the PFD/STR calculations for the models, are included in Appendix A. The graphics in Appendix A use the following symbols: circle for sensors and final elements; triangle for input and output modules; and rectangle for logic solvers. A standard symbol is used for relays, to clearly show connections to coils and contacts. The PFD and STR figures of the Simplified Models are listed in Table A1 of Appendix A. The figures in this table show relative values, not absolute values. This makes the comparison between configurations of each group easier. The base model in each group, i.e. the model with the smallest PFD and STR within the group, is highlighted as '(base)', and the PFD and STR figures of the other models are indicated in comparison to the ones of the base model.

The following assumptions apply to the Simplified Models throughout this section:

- Trip command is always de-energize to trip.
- Output module is of digital type (i.e. the output signal can be either 0 or an active voltage, L+).
- Final element is de-energize to close, and the process is safe when the final element is closed.
- A proof test interval of 12 months is considered for calculating PFD_{avg}.
- Systematic Capability (IEC, 2011b) of SIS components is not included in the analysis.
- Safety requirements, such as Hardware Fault Tolerance (HFT) and Common Cause Failure (CCF) (IEC, 2011a), are not intended to be addressed for the Simplified Models.
- No particular target SIL is used to judge the models against; the models are instead compared against each other, focusing on architectural differences.
- The simplified formulas given in (Smith, 2011) and (ISA, 2002) are used for calculating PFD and STR values respectively. See PFD formulas of IEC 61508 in (IEC, 2011c).
- The term PFD_{avg} is simplified to 'PFD' throughout this section and in Appendix A. As an example, PFD_B refers to PFD_{avg} of Model B. Similarly STR_W refers to the Spurious Trip Rate of Model W.

2.1. *Configurations with one SIS logic solver*

Let us begin with the simplest configuration: the classic SIS architecture with one logic solver, one sensor and one final element. As shown in Model A (see Appendix A), sensor S1 is wired to the SIS input module I1 to read the process variable (e.g. pressure or temperature). Logic solver LS1 receives input from I1, processes the safety logic, and initiates a trip signal to the output module O1, which in turn closes the final element F by depowering its output channel.

By using the simplified formulas (Smith, 2011; ISA, 2002) and applying the typical failure rates given in Table A2 for S1, I1, LS1, O1 and F (see Appendix A), the overall PFD and STR for Model A can be calculated to be:

$$PFD_A = 1.17E-03, \quad STR_A = 1.33E-06$$

In some applications the interface between the output modules and the final elements is established through interposing relays. Model B shows a modified form of Model A in which the trip command from output module O1 de-energizes the safety relay K1, and the relay then cuts the power to the final element F.

Interposing relays may be utilized for various reasons, such as current rating compatibility, electrical isolation preferences, separation of scope of supply, and ease of validation and testing. Interposing relays with multiple contacts may also be used as a means to interface between multiple sources of trip signals. However, utilizing interposing relays induces some